

IMPLEMENTASI ALGORITMA ELGAMAL DALAM MENJAGA KEASLIAN DOKUMEN DIGITAL

Rospita Sihombing¹, Amru Yasir², Welnof Satria³

1,2,3) Teknologi Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Dharmawangsa Medan, Indonesia

Article Info

Article history:

Received: 15 April 2024

Revised: 23 April 2024

Accepted: 29 April 2024

ABSTRACT

Abstrak

Saat ini dokumen dapat disimpan dalam bentuk digital bukan hanya dokumen dalam bentuk teks, tetapi dalam bentuk lainnya seperti foto, suara, video ataupun file-file lainnya. Kemudahan dalam hal pengarsipan dan distribusi, menyebabkan penggunaan dokumen digital menjadi pilihan utama untuk menyimpan informasi. Untuk menjaga keaslian dan originalitas suatu dokumen digital, dokumen digital dapat diaplikasikan pada dokumen tersebut. dokumen digital dan konvensional mempunyai fungsi yang sama yaitu menjaga keaslian dan kepemilikan dokumen. dokumen digital tidak berbentuk coretan tinta seperti pada dokumen konvensional. Pada bentuk dokumen digital berupa kombinasi dari kumpulan angka dan huruf unik yang disisipkan ke dalam seluruh isi dokumen digital. Dokumen digital dapat dibuat dengan menerapkan ilmu kriptografi. Dokumen digital dibuat melalui dua proses utama, yaitu proses signing untuk pembuatan kunci dan implementasinya ke dalam dokumen digital serta proses verifikasi yang digunakan untuk membandingkan Dokumen digital dengan file yang diterima. Salah satu algoritma yang dapat digunakan untuk membentuk Dokumen digital adalah algoritma ElGamal.

Kata Kunci : Arsip, Dokumen Digital, Algoritma Elgamal.

Abstract

Nowadays, documents can be stored in digital form, not only documents in the form of text, but in other forms such as photos, sounds, videos or other files. The ease of archiving and distribution, causing the use of digital documents to be the main choice for storing information. To maintain the authenticity and originality of a digital document, digital documents can be applied to the document. digital and conventional documents have the same function of maintaining the authenticity and ownership of documents. digital documents are not in the form of ink strokes as in conventional documents. In the form of digital documents in the form of a combination of a unique set of numbers and letters that are inserted into the entire contents of the digital document.

Digital documents can be created by applying the science of cryptography. Digital documents are created through two main processes, namely the signing process for key generation and implementation into digital documents and the verification process used to compare digital documents with received files. One of the algorithms that can be used to form digital documents is the ElGamal algorithm.

Keywords: *Archives, Digital Documents, Elgamal Algorithm.*

Djtechno: Jurnal Teknologi Informasi oleh Universitas Dharmawangsa Artikel ini bersifat open access yang didistribusikan di bawah syarat dan ketentuan dengan Lisensi Internasional Creative Commons Attribution NonCommercial ShareAlike 4.0 ([CC-BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/)).



Corresponding Author:

E-mail : sihombing_ropita@ymail.com

1. PENDAHULUAN

Untuk menjaga keaslian dan originalitas suatu dokumen digital, dokumen digital dapat diaplikasikan pada dokumen tersebut. dokumen digital dan konvensional mempunyai fungsi yang sama yaitu menjaga keaslian dan kepemilikan dokumen. dokumen digital tidak berbentuk coretan tinta seperti pada dokumen konvensional.

Pada bentuk dokumen digital berupa kombinasi dari kumpulan angka dan huruf unik yang disisipkan ke dalam seluruh isi dokumen digital. Dokumen digital dapat digunakan untuk mencegah penyangkalan kepemilikan dokumen, menjaga keaslian dan otentikasi pemilik.

Dokumen digital dapat dibuat dengan menerapkan ilmu kriptografi. Dokumen digital dibuat melalui dua proses utama, yaitu proses *signing* untuk pembuatan kunci dan implementasinya ke dalam dokumen digital serta proses verifikasi yang digunakan untuk membandingkan Dokumen digital dengan file yang diterima.

2. METODE PENELITIAN

Observasi, data dikumpulkan dari pengamatan dan pencatatan tentang cara pengarsipan dan penentuan keabsahan dokumen, baik secara digital maupun konvensional.

Studi kepustakaan, pengumpulan data melalui buku-buku tentang kriptografi, pengamanan file digital dan tanda tangan digital. Studi dokumentasi, pengumpulan data dilakukan melalui studi dari literatur literatur, jurnal-jurnal, artikel *online* yang sudah memiliki standar ISSN mengenai kriptografi, dokumen digital dan tanda tangan digital. Sistem dapat melakukan proses enkripsi pesan berupa *plaintext* yang diinputkan oleh *user*. Sistem dapat melakukan proses dekripsi untuk mengembalikan pesan asli yang telah terenkripsi. Sistem dapat mengubah *plaintext* menjadi *ciphertext* dari proses enkripsi. Dan mengembalikan *ciphertext* ke *plaintext* dengan proses dekripsi. Sistem dapat melakukan proses perhitungan enkripsi dan dekripsi kriptografi ElGamal.

3. HASIL DAN PEMBAHASAN

Tujuan dari analisa kebutuhan adalah untuk mendefinisikan apa yang harus dikerjakan oleh sistem, yaitu memenuhi keinginan pengguna/*user* untuk melakukan enkripsi dan dekripsi pada pesan atau informasi yang dimiliki.

ASCII control characters			ASCII printable characters			Extended ASCII characters										
00	NULL	(Null character)	32	space	54	@	96	-	128	C	160	À	192	L	224	Ô
01	SOH	(Start of Header)	33	!	55	A	97	a	129	U	161	Á	193	l	225	Õ
02	STX	(Start of Text)	34	"	56	B	98	b	130	à	162	Â	194		226	Ö
03	ETX	(End of Text)	35	#	57	C	99	c	131	á	163	Ã	195		227	Ø
04	EOT	(End of Trans.)	36	\$	58	D	100	d	132	ä	164	Ä	196		228	Ù
05	ENQ	(Enquiry)	37	%	59	E	101	e	133	å	165	Å	197		229	Ú
06	ACK	(Acknowledgement)	38	&	60	F	102	f	134	æ	166	Æ	198		230	Û
07	BEL	(Bell)	39	'	61	G	103	g	135	ç	167	Ç	199		231	Ü
08	BS	(Backspace)	40	(	62	H	104	h	136	è	168	È	200		232	Ý
09	HT	(Horizontal Tab)	41	)	63	I	105	i	137	é	169	É	201		233	Þ
10	LF	(Line feed)	42	*	64	J	106	j	138	ê	170	Ê	202		234	ß
11	VT	(Vertical Tab)	43	+	65	K	107	k	139	ë	171	Ë	203		235	Ü
12	FF	(Form feed)	44	,	66	L	108	l	140	ì	172	Ì	204		236	Ý
13	CR	(Carriage return)	45	-	67	M	109	m	141	í	173	Í	205		237	Þ
14	SO	(Shift Out)	46	.	68	N	110	n	142	î	174	Î	206		238	ß
15	SI	(Shift In)	47	/	69	O	111	o	143	ï	175	Ï	207		239	À
16	DLE	(Data link escape)	48	0	70	P	112	p	144		176		208		240	Á
17	DC1	(Device control 1)	49	1	71	Q	113	q	145		177		209		241	Â
18	DC2	(Device control 2)	50	2	72	R	114	r	146		178		210		242	Ã
19	DC3	(Device control 3)	51	3	73	S	115	s	147		179		211	¡	243	Ä
20	DC4	(Device control 4)	52	4	74	T	116	t	148		180		212	¢	244	Å
21	NAK	(Negative acknowl.)	53	5	75	U	117	u	149		181		213	£	245	Æ
22	SYN	(Synchronous idle)	54	6	76	V	118	v	150		182		214	¤	246	Ç
23	ETB	(End of trans. block)	55	7	77	W	119	w	151		183		215	¥	247	À
24	CAN	(Cancel)	56	8	78	X	120	x	152		184		216	¦	248	É
25	EM	(End of medium)	57	9	79	Y	121	y	153		185		217	§	249	Ê
26	SUB	(Substitute)	58	:	80	Z	122	z	154		186		218	¨	250	Ë
27	ESC	(Escape)	59	;	81	[	123	[	155		187		219	©	251	Ì
28	FS	(File separator)	60	<	82	\	124	\	156		188		220	ª	252	Í
29	GS	(Group separator)	61	=	83	]	125	]	157		189		221	«	253	Î
30	RS	(Record separator)	62	>	84	^	126	~	158		190		222	¬	254	Ï
31	US	(Unit separator)	63	?	85	_			159		191		223	­	255	nbsp

Gambar 3.2 Tabel Kode ASCII

Contoh Kasus :

Rospita akan mengirim pesan “ selamat Pagi “ Kepada Badriah melalui Kartika. Rospita tidak ingin pesan tersebut diketahui oleh badriah maka rospita mengenkripsi pesan tersebut untuk sampai kepada kartika (Private key) untuk proses deskripsi kepada badriah melalui kartika.

Penyelesaian perhitungan manula enkripsi dengan metode Elgamal sebagai berikut :

1. Pembentukan kunci

Siti membangkitkan pasangan kunci dengan memilih

bilangan : $p = 787$ $g = 185$ $x = 32$

Kemudian p, g, x digunakan untuk menghitung y :

$$y = g^x \bmod p$$

$$y = 185^{32} \bmod 787$$

$$y = 754$$

jadi kunci public yang dimiliki Siti adalah $y = 754, g = 185, p = 787$ dan kunci private yang akan dikirim kepada Nunuy untuk proses dekripsi adalah $x = 32, p = 787$

2. Enkripsi Pesan

Nilai ASCII dari pesan "Selamat PAGI" adalah 83 101 108 97 109 97 116 32 80 65 71 73

Kemudian nilai ASCII tersebut dimasukkan kedalam blok-blok nilai m secara Berurutan.

4. SIMPULAN

Berdasarkan hasil pembahasan dapat disimpulkan beberapa hal sebagai berikut:

Telah dihasilkan suatu aplikasi untuk penandaan dokumen dengan proses enkripsi dan deskripsi. Proses pengujian aplikasi menggunakan metode *Elgamal*, hasilnya adalah proses enkripsi dan deskripsi. mplementasi program ini menghasilkan suatu aplikasi yang dapat mengubah dokumen untuk menandai bahwasanya dokumen tersebut telah diamankan. Aplikasi disini hanya menandakan dokumen telah di enkripsi. Dan belum memproteksi dokumen.

UCAPAN TERIMA KASIH

Puji dan syukur Kepada Tuhan Yesus, yang telah memberikan kesehatan dan nafas kehidupan sampai saat ini, sehingga pada akhirnya penulis dapat menyelesaikan skripsi ini dengan baik. Terimakasih untuk orangtua saya yang menjadi pendukung dalam bentuk finansial dan mendoakan selama penulis menyusun skripsi. Terimakasih untuk kekasih saya yang selalu memberikan semangat dan doanya. Terimakasih untuk para pamong yang selalu memberikan nasehat dan semangat. Terimakasih untuk para Dosen Pembina dan Pembimbing yang membantu penulis dalam menyelesaikan skripsi.

PUSTAKA

- Ariyus. (2013). Kemanan Data. Retrieved June 30, 2018, from [http://repository.usu.ac.id/bitstream/handle/123456789/39071/Chapter II.pdf?sequence=4&isAllowed=y](http://repository.usu.ac.id/bitstream/handle/123456789/39071/Chapter%20II.pdf?sequence=4&isAllowed=y)
- A.S, R., & Shalahudin. (2014). Metode Waterfall. Retrieved June 28, 2018, from [http://eprints.polsri.ac.id/2203/3/BAB II.pdf](http://eprints.polsri.ac.id/2203/3/BAB%20II.pdf)
- Bunafit. (2013). Pengertian MYSQL. Retrieved June 25, 2018, from [http://eprints.polsri.ac.id/1082/3/BAB II.pdf](http://eprints.polsri.ac.id/1082/3/BAB%20II.pdf)
- Imaniawan, F. F. D., & Wati, F. F. (2017). Sistem Informasi Administrasi Kependudukan Berbasis Web Pada Desa Bogangin Sumpiuh. *Indonesian Journal on Networking and Security*, 7. Retrieved from ijns.org/journal/index.php/ijns/article/download/1516/1472
- Indrawati, Hartatik, S., & Utami, I. G. (2013). Penerapan Enkripsi Dan Deskripsi Menggunakan Algoritma Rc4. Retrieved June 30, 2018, from https://www.academia.edu/22370187/Penerapan_Enkripsi_Dan_Deskripsi_Menggunakan_Algoritma_Rc4
- Indrajani. (2015). Pengertian Basis Data. Retrieved May 20, 2018, from [http://library.binus.ac.id/eColls/eThesisdoc/Bab2/2014-2-00296-IF Bab2001.pdf](http://library.binus.ac.id/eColls/eThesisdoc/Bab2/2014-2-00296-IF%20Bab2001.pdf)
- L, I. (2017). Pengertian Kriptografi. Retrieved June 20, 2018, from <https://pojokteknologi.com/item/140-kriptografi>
- Lestari. (2013). Pengertian LRS. Retrieved June 30, 2018, from <http://repository.nusamandiri.ac.id/index.php/unduh/item/1836/10-BAB-II-landasan-teori.pdf>
- Prayitno, A., & Safitri, Y. (2015). Pemanfaatan Sistem Informasi Perpustakaan Digital Berbasis Website Untuk Para Penulis. *IJSE – Indonesian Journal on Software Engineering*, 1(1), 1–10.
- Rizaniar, F. N., & Sardiarinto. (2015). Perancangan Sistem Informasi Wisata Air Di Daerah Istimewa Yogyakarta Berbasis Web. Retrieved August 30, 2016, from <https://ejournal.bsi.ac.id/ejurnal/index.php/evolusi/article/view/625/516>

- Sukmaindrayana, A., & Sidik, R. (2017). Jurnal Manajemen. *Sistem Informasi Akademik Sekolah Berbasis Web Di Sekolah Menengah Pertama Negeri 11 Tasikmalaya*, 4(2), 1-158.
<https://doi.org/10.1017/CBO9781107415324.004>
- Sukmaindyarana, A., & Sidik, R. (2017). Aplikasi Grosir Pada Toko RsidikBungursari Tasikmalaya.
- Triase. (2015). Kriptografi-Elgamal-Menggunakan-Metode-Mersenne. Retrieved June 30, 2018, from https://www.researchgate.net/profile/Triase_St_Mkom/publication/319181684_Kriptografi_Elgamal_Menggunakan_Metode_Mersenne/Links/599872eaa6fdcc2615843d09/Kriptografi_Elgamal-Menggunakan-Metode-Mersenne.pdf?origin=publication_detail